Remarks

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-11, 15-73 and 80-85 are pending. Claim 1 and 61 are amended herein.

Statement of Substance of Interview Dated 12/11/2007

Applicant wishes to thank Examiner Robert Timblin for conducting a telephonic interview with Applicant's attorney, Daniel T. McGinnity, on 12/11/2007.

During the interview, Applicant's attorney discussed the differences between the cited references, Stone and Bush, and the claimed subject matter. In particular, it Applicant's attorney asserted that Stone is directed at administrative access to resources and is silent as to an operation to change multiple usernames and passwords to a cited references lack at least "performing an administrative password operation on a password associated with each of the selected multiple data sources to collectively update each said password to the new password", and "calls for custom logic, from a custom logic source outside the identity integration system" as recited for example in claim 1. For at least this reason, Applicant submits that the Office has not established a *prima facie* case of anticipation or obviousness for the pending claims. The Examiner acknowledged the differences between Stone and the subject matter of the application, but asserted that the differences were not clearly recited in at least some of the claims.

Accordingly, in the interest of expediting allowance of the application and without conceding the propriety of the rejection, Applicant's attorney proposed amendments to further clarify claimed features of claim 1. Applicant's attorney understood the Examiner to tentatively agree that the proposed amendments would overcome the outstanding rejections based on Stone. The Examiner indicated that the proposed amendments would need to be presented in writing and that the search would need to be updated.

Accordingly, amendments have been made to claims 1 herein in the spirit of those discussed during the interview. The remaining independent claims as previously presented include similar features, in varying terms and scope. Accordingly, Applicant has presented arguments with respect to these claims that are consistent with the differences acknowledged by the Examiner during the interview. Applicant submits that all of the pending claims are in condition for allowance. If any issues remain that would prevent the allowance of the application, Applicant requests that the Examiner contact the undersigned attorney to resolve the issues.

35 U.S.C. §101 Rejections

Claim 61 and its respective dependent claims are rejected under 35 U.S.C. §101 as directed to software per se. Appropriate correction is made herein. Accordingly, the §101 rejections have been obviated.

35 U.S.C. §102 and §103 Rejections

Claims 1-11,15-20, 22-26, 28-69, 71-73 and 80-85 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application No 2003/0233439 to Stone et al. ("Stone").

Claims 21 and 70 are rejected under 35 U.S.C. § 103(a) as unpatentable over Hu in view of U.S. Patent Application No. 2002/0083012 to Bush et al. ("Bush").

Claim 27 is rejected under 35 U.S.C. § 103(a) as unpatentable over Stone in view of Bush and in further view of US Patent No. 6,976,262 to Davis et al. ("Davis"). Applicant respectfully disagrees.

As discussed in the interview, Stone lacks at least operations to perform updating of credentials of a user (username/password) with multiple service providers to the same password as in the claims as presently recited. Stone does discuss separately (1) using separate user identifiers/passwords with different services and (2) using a single global identifier for an administrator to have access to the resources represented by the user identifiers/passwords. *See Stone [0066]-[0070].* Thus, Stone is directed at administrative accounts which may use a single global password. However, Stone does not discuss changing, updating or otherwise managing multiple user accounts/passwords associated with the same user.

Thus, part of what Stone lacks relative the recited claims is an operation to change username/password maintained with different services for a user to the

same username/password through a common interface. Stone is silent as to such common setting of user passwords with different services/resources. Rather than addressing user access to resources, Stone is concerned with an administrator's access to manage the resources. To do so, Stone provides the administrator with an administrative account that has access to all the resources. Moreover, this is a single administrative account that has a single set of credentials, e.g., global identifier/password. Accordingly, setting the global identifier/password (singular) is not equivalent to changing multiple user credentials with multiple providers to the same credentials as in the presently recited claims. For example:

Claim 53 recites as previously presented recites an apparatus comprising:

- a processor; and
- a web application for password management executable on the processor having one or more modules including:
    - a user identifier to find user identity information in an identity integration system, wherein:
        - the identity integration system includes a management agent for each of multiple data sources to manage data communication between the identity integration system and each respective data source; and
        - for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;
    - ***identity information query logic to search information in the identity integration system for accounts associated with the user***;
    - ***an account lister to display the accounts associated with the user***;
    - ***an account selector to designate at least some of the displayed accounts for password management***;
    - **a password inputter to determine a new password input by a user to associate with each designated accounts**; and

- ***a password manager to collectively manage passwords*** for the designated accounts by requesting ***an update of a password associated with each designated account to the new password,*** responsive to the user input.

(emphasis added).

In rejecting claim 53, the Examiner relies upon Stone paragraph [0071] for a global password which the Examiner equates to "a password manager to collectively manage passwords for the designated accounts by requesting an update of a password associated with each designated account to the new password, responsive to the user input" as in claim 53. *Office Action, p. 14.* Applicant respectfully disagrees.

As noted previously, the global password of Stone is a singular password that is used to gain administrative access via a single administrative account. While the administrative account may be permitted access to many resources, using a single administrative account to administer many resources is different than collectively managing multiple user accounts and associated credentials for a user. As such, Stone does not provide a basis for "a password manager to collectively manage passwords for the designated accounts" as in claim 53, e.g., multiple accounts selected by a user for password management. Further, Stone lacks by "requesting an update of a password associated with each designated account to the new password, responsive to the user input" as also recited in claim 53. Nor does Stone provide a basis for "a password inputter to determine a new password input by a user to associate with each designated accounts" as further

recited in claim 53. Again, while Stone may use a global password to gain access to different resources and/or to represent different sets of user identifiers, Stone does not discuss providing capability for a password to be input by a user to set a password for multiple designated accounts, as contemplated by in claim 53.

In addition, as Stone is limited to administrative access to resources and does not address user management of accounts, Stone is also silent as to "identity information query logic to search information in the identity integration system for accounts associated with the user" and "an account lister to display the accounts associated with the user". For the recited "query logic" feature, the Examiner in the Office Action p. 14 cites to Stone paragraph [0078] which merely describes a personalized web page that may present resources associated with an account to which a user is authenticated. However, paragraph [0078] is silent as to searching for and/or presenting multiple different accounts that are associated with a user. Thus, the recited feature is lacking in Stone.

For the recited "account lister" feature, the Examiner in the Office Action p. 14 cites to Stone paragraph [0017] which merely describes:

> In accordance with the invention, FIG. 1 shows a block diagram of a client-server data processing system 10 or a network. The client-server data processing system 10 includes a central administration tool 14 for administering maintenance and operation for one or more clients 46 that seek access to one or more resources (e.g., 36 and 50) via an internal network 44 or another communications network. A central administration tool 14 communicates with a server 26 via a communications network 22 (e.g., the Internet). A user interface 12 is coupled to the central administration tool 14 to support an administrator's entry or selection of information

> such as attributes of users, attributes of groups, attributes of resources, attributes of objects, access of users or groups to resources, configurations, or other data associated with operations and maintenance of the client-server data processing system 10. *Stone, paragraph [0017].*

Respectfully, the Applicant does not see how the Examiner arrives at the recited "account lister to display the accounts associated with the user" from the description in paragraph [0017]. An administrative tool to set administrative attributes, as is discussed in the above excerpt from Stone, is not equivalent to an account lister that presents multiple accounts associated with a user that are arrived at through query logic that search an identify integration system. Stone is simply silent as to this recited feature of claim 53.

Likewise, Stone fails to provide "an account selector to designate at least some of the displayed accounts for password management;" For the recited "account selector" feature, the Examiner in the Office Action p. 14 cites to Stone paragraph [0053] which merely describes:

> In step S18, the directory services system invokes an action consistent with the contents of the file. In one example, the action may comprise definition, modification, deletion, or addition of an attribute or an attribute value to the directory services system 32. In another example, the action may comprise one or more of the following activities: management of security measures for one or more users; provision of access to software programs, features, or capabilities for one or more users; and the management of resources for one or more users. *Stone, paragraph [0053].*

Again the Applicant does not see what in paragraph [0053] the Examiner interprets as the recited "account selector". There is no mention in the above excerpt of accounts, listing of a set of accounts, or selection of accounts. The above except describes using attributes to set security, access, capabilities and so forth, which may be considered as administrative management to specify which resources are available to one or more users through their individual accounts. However, individually managing resources available to a user as in Stone is not equivalent to providing a user the capability to collectively manage multiple accounts of the user. Moreover, Stone does not in paragraph [0053] or elsewhere discuss an account selector through which a user may designate accounts for password management". Stone is simply silent as to this recited feature.

While Stone mentions users identifiers/password which for arguments sake may be considered accounts, Stone does not in paragraphs [0078], [0017], [0053] or elsewhere describe techniques to manage, set, update or change the user identifiers/passwords at all, let alone collectively managing, setting, or updating passwords for multiple accounts via a web application, query logic, account lister, account selector, and so forth as in claim 53. Claim 53 and it respective dependent claims are allowable for at least the foregoing reasons and withdrawal of the §102 rejection is respectfully requested.

In the interest of expediting allowance of the subject application and without conceding the propriety of the rejections, amendments have been made to claim 1 in the spirit of those discussed during the interview. For example,

Claim 1 as amended recites a method, comprising:

- ***outputting a user interface configured to interact with an identity integration system to perform collective password management for multiple user accounts associated with a user;***
- ***receiving a selection of multiple data sources connected to the identity integration system input by the user via the user interface, wherein:***
  - ***each of the multiple data sources corresponds to a different one of said multiple user accounts;***
  - the identity integration system includes a management agent for each of the multiple data sources configured specifically for its respective data source to manage data communication between the identity integration system and each respective data source;
  - for at least some of the multiple data sources a management agent for the data source is configured with credentials to perform password management for a corresponding said user account; and
  - for at least one of the multiple data sources a management agent for the data source calls for custom logic configured as code, from a custom logic source outside the identity integration system, to perform password management for the data source;
- ***receiving a new password input by a user via the user interface***; and
- ***performing an administrative password operation on multiple passwords each associated with one of the selected multiple data sources to collectively update each of the multiple passwords to the new password, wherein the password operation is performed using the identity integration system.***

Applicant understood the Examiner as agreeing in the interview of 12/11/07 that Stone was directed to techniques involving using a single administrative account and a global password to access resources and set attributes for user accounts. For reasons discussed with respect to claim 53, Stone does not disclose, teach, or suggest collective password operations, updates, or administrative password management related to multiple accounts of a user. Further, Stone is

silent as to collectively managing by a user of passwords associated with multiple different accounts of the user.

For similar reasons, Stone lacks "outputting a user interface configured to interact with an identity integration system to perform collective password management for multiple user accounts associated with a user" as presently recited in claim 1. Stone expresses no concern for collective password management of multiple user accounts by a user. Likewise, Stone fails to provide a basis for "receiving a selection of multiple data sources connected to the identity integration system input by the user via the user interface". No such selection of data sources or accounts by a user from among multiple accounts is discussed in Stone.

Moreover, Stone does not provide any basis for the presently recited features of (1) "receiving a new password input by a user via the user interface" and (2) "performing an administrative password operation on multiple passwords each associated with one of the selected multiple data sources to collectively update each of the multiple passwords to the new password, wherein the password operation is performed using the identity integration system".

Stone simply does not discuss a user input of a password via a user interface to perform password management. More particularly, for reasons discussed in detail with respect to claim 53, Stone lacks collectively updating "each of" multiple passwords associated with multiple passwords to a "new password" input by a user. In other words, in the claimed techniques a user may select multiple accounts and input a new password via the user interface. Then the

identity integration system changes passwords with as many accounts of the user as are selected to the input new password. Techniques described in Stone, such as setting of a single global password, are not equivalent to these recited features of claim 1. Stone does not disclose, teach, or suggest password operations performed collectively on multiple passwords of multiple data sources. Accordingly, claim 1 is allowable for at least these reasons and withdrawal of the §102 rejection is respectfully requested.

Claims 2-11 and **15-52** depend either directly or indirectly from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither shown nor suggested in the references of record.

Each of the remaining independent claims 61, 65, 80 and 82 recite features similar to claims 53 and 1 in varying terms and scope. For example:

Claim 61 recites in part:

- logic for communicating with the identity integration system, wherein:
  - the identity integration system is capable of **collectively updating a password on multiple data sources** that use various functions of password updating ***responsive to input of a single new password by a user***;

Claim 65 recites in part:

- a web application for producing a list of the accounts from the identity integration system, for allowing selection of at least some of the accounts, ***for inputting by a user of a new password to cause the new password to be associated with each of the selected accounts,*** and for requesting the identity integration system to ***collectively update passwords on each of the selected accounts to the input new password;***

Claim 80 recites in part:

- ***allowing input of a new password via the user interface selection device; and***
- ***allowing input of a request to update old passwords associated with each of the selected accounts to the new password input via the user interface.***

Claim 82 recites in part:

- ***receiving a new password input by a user to cause the new password to be associated with each of the selected multiple data sources; and***
- using the identity integration system to ***collectively update a password associated with each of the selected multiple data sources to the new password input by the user***

Thus, each of claims 61, 65, 80, and 82 contemplates collective management/updating of multiple passwords for multiple data sources. As discussed with respect to claims 53 and 1, Stone does not disclose, teach or suggest collective password operations, updates, or administrative password management related to multiple accounts of a user. Stone for example is directed at using an administrative account to access many resources and to set attributes for user accounts. However, Stone is silent as to collectively managing by a user of passwords associated with multiple different accounts of the user. Bush and Davis are cited for a help desk and a management interface respectively, and do not correct the noted defects in Stone. Accordingly, claims 61, 65, 80, and 82 and their respective dependent claims are allowable based on similar reasoning and withdrawal of the §102 and §103 rejections is respectfully requested.

Conclusion

The Application is in condition for allowance and the Applicant respectfully requests reconsideration and issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is requested to contact the undersigned attorney to discuss the unresolved issue.

Respectfully submitted,

Date: 1/22/08

By: /Daniel T. McGinnity, #55444/

Daniel T. McGinnity
Reg. No. 55444
Attorney for Applicant

Sadler, Breen, Morasch & Colby, PS
422 W. Riverside Avenue, Suite 424
Spokane, Washington 99201
Telephone: (509) 755-7257
Facsimile: (509) 755-7252